Tatjana Gerginova

The Concept of Security and Hybrid Threats

Abstract

In theoretical terms, there is no single definition of the concept of security. The concept of security is shaped by values, threats, challenges and risks that appear in different forms and are defined in different contexts. Hence, we can talk about national security, social security, health security, society security, occupational security, traffic security, etc. Modern globalisation has caused an increase in security threats and risks. This process continuously produces a series of economic and social inequalities for most of the world's population, but also various forms of geopolitical competition, exploitation of countries and discrimination of people. Within the framework of the paper, the author will define the term "Concept of Security" and analyse the terms "asymmetric threats", "hybrid threats" and "building resistance". In the final part of the paper, the author states the following conclusions: Globalisation is the driver and creator of new modified risks; therefore, it is difficult to draw a line of separation between threats and security risks. Modern modified risks are not selective – on the contrary, they affect all countries and social classes and have global consequences. The new types of threats are multiplied and transnational and require a wide range of instruments to deal with them. The content will be created based on the analysis of foreign literature and using electronic content. In preparing the content of the paper, the author will apply the general scientific methods: the descriptive method, normative method, comparative method and content analysis method as a special scientific method.

Keywords: concept of security, asymmetric threats, hybrid threats, building resilience

DOI: https://doi.org/10.36250/01260_12

Introduction

Security is essentially a changing category and therefore its understanding is determined by many different factors, such us: new security threats and risks, new security actors, new security responses, new security needs and interests and changing dynamics in international relations.

The modern world faces the following threats: traditional (military) and modern (non-military) threats that must be prevented and defended collectively, by applying a mutual set of traditional and new approaches and methods. Modern threats are multiplied and transnational and require a wide range of instruments to deal with them. They are not selective – on the contrary, they affect all countries and social classes and have global consequences.

It follows from this that the concept of security has an evolutionary character and is therefore subject to continuous change and development in the context of the specifics of the security environment. In this regard, the importance of non-military security threats and risks is a specific feature of contemporary security understanding. As a result, concepts such as environmental security, food security, energy security, etc. appear on the security agenda.

Security in the modern world

In the 21st century, security is facing a deep transformation, the emphasis is shifting from threats to risks and this leads to a different perception of security. The complexity arises from the fact that modern risks differ in many aspects from the past, they are unpredictable and it is difficult to determine their causes, origins and the effects they can cause.

As a result of this, authors appear in the scientific literature according to which the concept of global security is closely related to the concept of a global risk society. According to these authors, risks come without warning, have their own temporal manifestation (do not wait), have no specific timing or location.

These concepts contribute to a more extensive consideration of the security aspects that are related to the new circumstances resulting from the modified risks, which can easily lead to global chaos and disorder.

In the scientific literature, there is agreement that safety is a variable category that is determined by many factors and processes. As a result, security perceptions and concepts are defined in different contexts.

If analysed from the aspect of political, scientific-technological and socio-economic problems, the acquisition of security in the modern world is a complex endeavour (Gerginova 2023).

With that in mind, security is a complicated, multi factorial and hierarchical phenomenon. Its analysis and understanding should also have an interdisciplinary character. This is because of the changing nature of security.

The basis of security consists in arranging conditions for existence, survival in the present time and advancement in the future. Ensuring this condition implies the ability of social entities to eliminate the threats that have been defined. In situations of asymmetric security, threats are not always clearly defined. They often consist of their own system structures, in the relations and status of the subjects of international relations. The imbalance, the mismatch have political, military, economic, legal, social and societal dimensions, which further exacerbate the complexity of today's security environment.

As a result, new security concepts are emerging, such as environmental security, economic security, energy security, societal security, critical infrastructure security, social security, health security, society security, occupational security, traffic security, cybersecurity, etc. These new security concepts initiate increased attention in security research and the security agenda, while the reasons for them are mainly related to the increased frequency of non-traditional threats and risks.

The term asymmetric threats

According to certain authors, asymmetry is an integral part of the history of society and warfare, that is, asymmetric issues have a history as long as humanity (Metz–Johnson 2001).

Asymmetric warfare and its conceptual basis are particularly visible in the writings of Sun Tzu, while the basic concept of asymmetric warfare is a model by which the technologically and numerically weaker opponent enables inflicting losses on the opposite side, presenting results in order to promote its views and goals, and by striving to motivate new like-minded people.

A broader consideration of the nature of asymmetric threats implies the development and application of security threat methods that are different from the assumed concepts or tactics and doctrine applied by the adversary.

Asymmetry in defence and security can be traced through the pronounced disproportion in the development and possession of military technology, as there are many examples in the history of warfare during the 20th century. Also, asymmetry can be monitored from the point of view of disproportionately expressed fighting will, population support and fighting morale of the opposing sides. Organisational symmetry can also be of great importance and in individual cases it can contribute to partial compensation of technological asymmetry.

Certain authors point to an asymmetry in patience, perseverance and time perspectives, which is particularly significant in conflicts between opposing parties who have different cultural perceptions of warfare (Metz–Johnson 2001).

There are several definitions with content for asymmetric threats, but in principle, the term is also used to describe the attack on institutions of states that do not have adequate equipment and the tactics of which are specific in form and expressed goals. Based on certain analyses, it is possible to conditionally determine the determinants of asymmetric warfare (Lambakis et al. 2002).

An asymmetric security threat is a new, surprising, unusual and unexpected threat. This threat is conditioned by the current historical security circumstances faced by the national institutions and by the position and attitudes of certain states according to the global foreign and security policy.

The general system of the state organisation shows latent institutional weaknesses in the current, classic way of responding to security threats and is predominantly aimed at preventing and deflecting consequences and less at prevention and building a protection system. The existence and application of new tactics and developed operational capabilities as well as technical and non-conventional means in the action of the adversary can be ascertained.

According to the time of implementation, asymmetric action can be short-term or long-term, as well as variable in terms of the use of methods, technology, organisation, etc. Also, any asymmetric operation can have a physical and psychological component.

According to the possible effects, asymmetric action can be defined as: effect according to the population (number of the affected population, degree of destructive effects of the affected population); economic effect (economic losses and degree of destruction of economic and service potential); environmental effects; political effects; psychological effects; public health consequences (Metz–Johnson 2001).

The term hybrid threats

The term hybrid threat refers to an action conducted by state or non-state actors, whose goal is to undermine or harm a target by influencing its decision-making at the local, regional, state or institutional level. Such actions are coordinated and synchronised and deliberately target the vulnerabilities of democratic states and institutions. Activities can take place, for example, in the political, economic, military, civil or information domains. They are conducted using a wide range of means and designed to remain below the threshold of detection and attribution (Hybrid CoE 2022).

The current transition in international power structures provides a fertile environment for hybrid action. The intensifying conflict of values between the West and authoritarian states erodes international norms and institutions making open Western societies targets for comprehensive hybrid action.

A conflict of values that extends to the domestic sphere of Western societies increases polarisation and disunity within and among Western actors, making them more vulnerable to external interference. Recent developments in modern technology and an increasingly complex information environment provide powerful instruments for hybrid actors if not properly countered by the Western community.

Hybrid warfare is based on the discovery of hybrid risks and the creation of hybrid threats to the security of a state, all in order to influence its weaknesses and enable the realisation of one's own interests, without (or with minimal) use of direct military power.[1]

The concept of hybrid warfare sublimates in itself a combination of conventional, unconventional, terrorist, criminal, psychological, economic, energy and other instruments for the destabilisation of the state, i.e. a combination of the use of illegal combat operations, sponsorship, organisation and implementation of political protests, economic measures, which are followed by strong information campaigns, psychological-propaganda activities, the misuse of various information, the use of social media (the Internet) for propaganda purposes, but also as a tool for radicalisation, financing, etc.

Hybrid warfare can be carried out by state or non-state entities, whereby it is mandatory that the engaged non-state actors have the support of a certain external state entity.

[1] See https://repository.ukim.mk/bitstream/20.500.12188/2308/1/acvetanovska2019_1.pdf

According to certain theories, hybrid warfare unites a whole spectrum of different models of warfare that are conducted with conventional, unconventional tactics and engaged forces, including violence and civil unrest, as well as criminal activity (Hoffman 2007).

Emergent forms of action can range from violent secessions or annexation of a part of the territory, overthrowing the government or changing the political system in a country.

All these and other aimed at destabilising the state or changing the government in it, are organised and implemented in order to achieve the strategic interests of the great powers or the isolated centres of power (corporation, internal groups) with the aim of determining the state of disruption of the balance of power in international relations and the realisation of one's own interests, mostly by non-combatant means (Kofman–Rojansky 2015).

In accordance with modern trends, new dimensions of conflicts are also emerging. The main dimension of hybrid warfare is covert subversive activity used against objects of aggression as the main means of destroying the enemy.

In the modern global environment, every national country determines the need for constant development of the national security policy and the ability to respond to changes, because external and internal challenges, risks and threats change continuously and rapidly and are very complex, they are connected and often unpredictable.

The strengthening of the power of non-state actors further complicates the security situation in the world. Changes in global power centres will affect a number of regional and local events and processes that can significantly affect national security challenges and threats. The geopolitical contest of the great powers influences the outbreak of interstate and intrastate conflicts.

Building national resilience is the primary responsibility of member states, because countering hybrid threats is about national security and defence.

Resilience is a national responsibility. Resilience is the ability of an individual, household, community, country or region to withstand, cope with, adapt to and quickly recover from stresses and shocks such as violence, conflict, drought and other natural disasters without jeopardising long-term development (European Commission 2016).

Conclusion

Today, every country should be able to adapt to the unpredictable, complex and changing security reality. This implies the need to build national capacities to improve resilience to these threats through a broader, more integrated and better coordination approach at the national level.

Today, many member states face common threats that can be more effectively addressed at the level of the European Union. The European Union can be used as a platform to strengthen national efforts and, through its regulatory capacity, establish common benchmarks that can help raise the level of protection and resilience across the EU.

The EU can therefore play an important role in improving our collective situational awareness, in building Member States' resilience to hybrid threats and in crisis prevention, response and recovery. Modern threats have a complex content, and therefore the need to respond to the entire society is imposed. Strengthening resilience requires a long-term approach based on mitigating the root causes that contribute to crises and strengthening capacities to better manage future uncertainty and change.

In relation to security, there is a resilience approach, which would identify and reduce vulnerabilities, and will minimise the effects of potential threats, which points to the importance of the capabilities of entities that have response and recovery actions. In order to ensure a comprehensive approach to the resilience of critical entities, each Member State should have a strategy for improving the resilience of critical entities. The strategy should set out the strategic objectives and policy measures to be implemented. When setting their strategies, Member States should take due account of the hybrid nature of threats to critical entities. The purpose of the Strategy for building resilience and dealing with hybrid threats is to create a common awareness of the nature of hybrid threats, mapping the obligations and bearers, identifying the ways of action, as well as creating resources for building national resilience by engaging the entire society.

If the three core methods (detection, rejection and response to threats) are accurately applied, national resilience and dealing with hybrid threats can be properly realised.

References

European Commission (2016): *Building Resilience: The EU's Approach.* Online: https://ec.europa.eu/echo/files/aid/countries/factsheets/thematic/EU_building_resilience_en.pdf

Gerginova, Tatjana (2023): *Global Security.* University St. Kliment Ohridski – Bitola, Faculty of Security, Skopje.

Hoffman, Frank (2007): *Conflict in the 21st Century: The Rise of Hybrid Wars.* Arlington: Potomac Institute for Policy Studies.

Hybrid CoE (2022): *Hybrid Threats as a Concept.* Online: www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/

Kofman, Michael – Rojansky, Matthew (2015): A Closer look at Russia's "Hybrid War". *Kennan Cable,* (7), 1–8. Online: www.files.ethz.ch/isn/190090/5-KENNAN%20CABLE-ROJANSKY%20KOFMAN.pdf

Lambakis, Steven – Kiras, James – Kolet, Kristin (2002): Understanding "Asymmetric" Threats to the United States. *Comparative Strategy,* 21(4), 241–277. Online: https://doi.org/10.1080/01495930290043065a

Metz, Steven – Johnson, Douglas V. (2001): *Asymmetry and U.S. Military Strategy: Definition, Background and Strategic Concepts.* Carlisle: U.S. Army War College Press. Online: https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=1120&context=monographs

Mitrović, Miroslav (2017): Hybrid Warfare and Asymmetric Security Threat. *Military Work,* 69(5), 333–347. Online: https://doi.org/10.5937/vojdelo1705333M